Tracking spam mails using SPRT algorithm with AAA

Deenashree M P[1], Spoorthi A[2], Johnpaul C I[3]

[1] B.E, Dept of ISE, NIE, Karnataka, India
[2] B.E, Dept of ISE, NIE, Karnataka, India

[3]Assistant Professor, Dept of ISE, NIE, Karnataka, India

---***---

Abstract— *A large number of compromised machines which are used to send spam mails have become a threat to organizations. There is increase in wastage of network bandwidth due to spamming. This has become a major challenge for administrators to identify and block the spammers in a network. Attack by Insiders has resulted in decreased reputation of the organization which is the major setback. Hence organizations need a system to validate users and to detect spam mails which is much needed in the society.*

Introduction

The E-mail traffic consists of unsolicited messages called Spam. Email spam, also known as junk email or unsolicited bulk email, is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware. Dealing with Spam incurs high costs for organizations, prompting efforts to try to reduce spam related costs by installing Spam Filters. Spamming causes wastage of network bandwidth.

Attacks by Insiders have caused major threat to the organizations. So it is a significant challenge for system administrators to identify and block the spammers in a network. Spamming provides a key for attackers to recruit the large number of compromised machines. A major security challenge on the internet is the existence of a large number of compromised machine which have been used to send spam mails and other security attacks including spamming and spreading malware, distributed denial of service(DDOS) attacks. Identifying and clearing compromised machines in a network remain a significant challenge for system administrators of network of all sizes.

Literature Survey

Based on email messages received at a large email service provider, two recent studies investigated the aggregate global characteristics of spamming botnets including the size of botnets and the spamming patterns of botnets[1]. These studies provided important insights into the aggregate global characteristics of spamming botnets by clustering spam messages received at the provider into spam campaigns using embedded URLs and near-duplicate content clustering, respectively. Given that spamming provides a key economic incentive for attackers to recruit the large number of compromised machines, we focus on the detection of the compromised machines in a network that are involved in the spamming activities, commonly known as spam zombies[1]. Recent studies show that SPOT is an effective and efficient system in automatically detecting compromised machines in a network [3]. When we compared spam detection algorithms, the performance of SPOT with two other spam zombie detection algorithms based on the number and percentage of spam messages forwarded by internal machines, respectively, it has been observed that SPOT outperforms those two detection algorithms [3]. In AAA concept, part of whose mechanism we are going to implement in our project, is said to be efficient for network management and security in a network[2]. In AAA system architecture, a set of security mechanisms for real-time secondary market services have been proposed. In this architecture[2], the issues of authenticating and authorizing secondary users, synchronizing a group of secondary devices, managing handoff, and detecting unauthorized spectrum usage are detected. A part of its mechanism is used in order to prevent unauthorized users from sending messages from the network.

Proposed system

Proposed system aims at the detection of the compromised machines in a network that are involved in the spamming activities, commonly known as spam zombies. It deletes email with attached viruses, detects and blocks the spam mails by using SPRT algorithm and generates a graph which gives the record of each individual spammer to know the frequency and probability.

Proposed system consists of Authentication server which uses authentication, authorization and accounting (AAA) concept. Authentication server verifies whether the user is authenticated and authorized to send the mail, accounting maintains the log of emails sent.

Mail server uses SPRT algorithm which detects spam mails andevery spam mail detected is blocked by the mail server but the spammer is notified that the mail has been sent. A record is maintained for every spam mail sent.

Consists of four modules: Staff machine, Authentication server, Mail server, Admin.

Staff Machine

Each user requests Authentication server for the registration. The request packet consists of User name, Mac Id, Ip address, Machine name, Date and time. Checks the request status from Authentication server either accepted or rejected. If accepted, a private key is generated else the reason for rejection is viewed to the user. As shown in Fig. 3.1 If the user is validated as authentic then he can login to the system successfully and send mails.

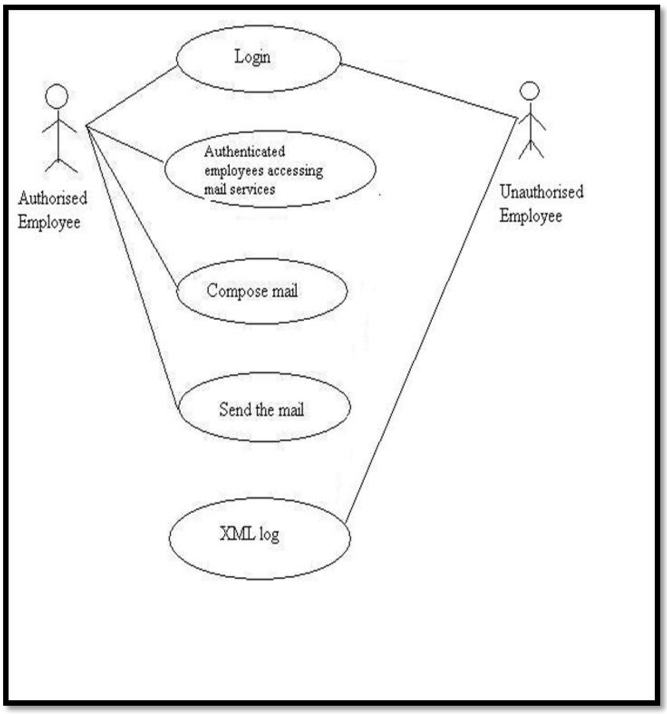

Fig. 3.1 Functionality of Authentication server and staff machine

Authentication server

Authentication server grants the request for registration if the staff machine's Mac Id, Ip address belongs to the same network and the user name, machine name are valid and gives a private key to that user. Authentication server also maintains user account. It stores user name, email id, password and "can send" (an option which tells if the user is authorized to send mail or not) in an xml file.

When the user tries to login, it checks for authenticity and if it is valid then the user can successfully login and it logs this login activity by storing the Mac ID, Ip address, machine name and user name in an xml file along with public and private key of that machine else it will reject with a reason.

Mail server

Mail server is a multithreaded server to receive mail packets and to forward to authentication server.

It consists of Background Processing :

a. Packet sniffer module: To capture each mail packet and identify source ip, packet data, packet size, packet length.
b. Packet analyzer: Received packets should be parsed to extract above information and display continuously on server screen.
c. Generate OTP and send to Authentication server: Authentication server encrypts OTP using public key stored during registration process and send to client. Client machine decrypts with private key and send back to Authentication server, if verified send TRUE to mail server and it forwards mail and maintain log, if false log is maintained to keep track of intruder. Monitors the number of mails received from each ip to find inflow packets from each client machine.

Admin

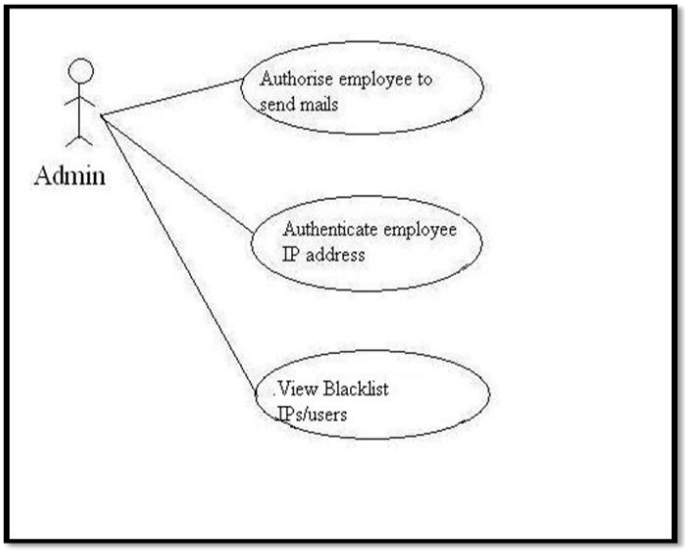
Admin
Authorise employee to send mails
Authenticate employee IP address
View Blacklist IPs/users

Fig. 3.2. Functionality of AAA

Process start or stop service, configures SMTP settings to send mail, maintains a view log (content log) sent by intruder, statistics report of each user as number of spam mails sent as shown in Fig.3.2.

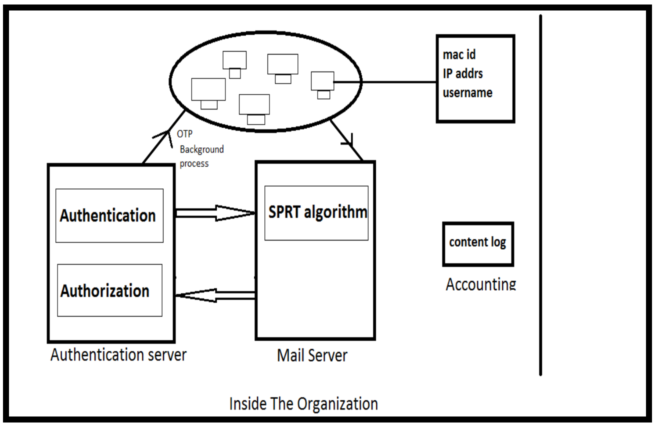

Fig. 3.3 Working

The overview and the working of the complete model is discussed in this paragraph. When the user logs in to the system, the mail is redirected to authentication server from the mail server for the account authentication and authorization of the user. The process is to request packets- Mac id, IP address, User name, Date and time. If the fields are valid, the account is authenticated and approved otherwise, rejected. The roles of logged in user- Is he eligible to send the mail? is checked. An OTP is generated to check for authorization. The next step is to detect if the mail is spam or not. For the same, in mail server SPRT algorithm is run. The system mails are applied to content based filtering process and pre-defined threshold values are considered to judge if the mails are spam or not. If the mails are spam then they are blocked in the mail server without the knowledge of the sender. A graph is recorded secretly with coordinates as ip address vs the frequency of spam mail generation. According to the graph generated the organization can take necessary action.

Conclusion

By plotting a graph the number of observations required can be minimized hence making it an effective and an efficient system. The graph contains IP address on x-axis and number of times the spam mails sent on y-axis. The system will work well in the environment of dynamic IP address. Spam mails which are sent using the name of an organization can be prevented. If an insider of an organization is generating the mails which he is not authorized/authenticated to send repeatedly, this system automatically generates a statistical analysis of the number of times the same person is repeating the process.

The AAA concept will authenticate, authorize and does accounting of the spam mails sent. There is an increase in efficiency of the system as the SPRT algorithm is not run unless the user is authenticated and therefore, protect the integrity and block the spam mails.

Future Scope

Threats from outside the organizations have increased so building a system that will monitor the spam mails coming from outside and blocking them such that the threats from outside the organization can be reduced. To build a system which will provide security for the insiders in any organization from receiving spam mails.

REFERENCES

[1] Zhenhai Duan, Senior Member, IEEE, Peng Chen, Fernando Sanchez, Yingfei Dong, Member, IEEE, Mary Stephenson, and James Michael Barker," Detecting Spam Zombies by Monitoring Outgoing Messages", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012.

[2] "On the architecture of Authentication, Authorization and Accounting for Real time secondary market services" Yihong Zhou, Dapeng Wu and Scott M. Nettles INTERNATIONAL JOURNAL OF WIRELESS AND MOBILE COMPUTING, JAN 2005.

[3] "Detecting Spam Zombies Using Spot Tool By Monitoring Outgoing Messages" INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING, Volume 3, Issue 4, April 2013.